AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A communication device requested for authentication for connection from another communication device, the communication device comprising:

a receiving section for receiving, from the another communication device, an authentication request including device information by which the another communication device is capable of ~~uniquely specifying the another communication device~~ being determined to be a source, and for monitoring and determining whether or not the authentication request is changed by an unspecified third party while being transmitted;

a display section for, when it is determined that the authentication request is not changed, displaying the device information included in the authentication request on a screen thereof;

an input section for receiving an input ~~instruction determined by a user based on the screen of the display section; and~~ of a confirmation result of the displayed device information from a user;

a transmission section for transmitting an authentication response including information indicative of verification or non-verification of the authentication with the another communication device in accordance with the result input to the input section; and

an authentication section for, ~~executing processing of verifying or not verifying the authentication with the another communication device in accordance with the instruction input to the input section~~ when the information included in the authentication response is indicative of verification of the authentication, performing key exchange with the another communication device using the device information included in the authentication request and the information

included in the authentication response.

2. (Currently Amended) A communication device requesting another communication device for authentication for connection, the communication device comprising:

a transmission section for transmitting an authentication request including device information indicative of ~~capable of uniquely specifying~~ the communication device to the another communication device;

a receiving section for receiving, from the another communication device, an authentication response corresponding to the authentication request and including device information ~~corresponding to the authentication request from the another communication device~~ by which the another communication device is capable of being determined to be a source, and for monitoring and determining whether or not the authentication response is changed by an unspecified third party while being transmitted;

a display section for, when it is determined that the authentication response is not changed, displaying the device information included in the authentication response on a screen thereof;

an input section for receiving an input ~~instruction determined by a user based on the screen of the display section~~ of a confirmation result of the displayed device information from a user; and

an authentication section for executing processing of verifying or not verifying the authentication with the another communication device in accordance with the result ~~instruction~~

input to the input section, and for, when the result is indicative of verification of the authentication, further performing key exchange with the another communication device using the device information included in the authentication request and the authentication response.

3-10. (Canceled)

11. (Currently Amended) A communication system for executing authentication processing for connecting a first communication device to a second communication device, wherein:

the first communication device includes:

a transmission section for transmitting an authentication request including device information by which the first communication device is capable of being determined to be a source ~~uniquely specifying the first communication device~~ to the second communication device;

a receiving section for receiving, from the second communication device, an authentication response corresponding to the authentication request and including device information ~~corresponding to the authentication request from the second communication device~~ indicative of verification or non-verification of the authentication with the first communication device, and for monitoring and determining whether or not the authentication response is changed by an unspecified third party while being transmitted; and

an authentication section for, when it is determined that the authentication response is not changed, executing processing of verifying or not verifying the authentication with the second communication device in accordance with the authentication response, and for,

when the device information included in the authentication response is indicative of verification of the authentication, further performing key exchange with the second communication device using the device information included in the authentication request and the authentication response; and

the second communication device includes:

a receiving section for receiving the authentication request from the first communication device, and for monitoring and determining whether or not the authentication request is changed by an unspecified third party while being transmitted;

a display section for, when it is determined that the authentication request is not changed, displaying the device information included in the authentication request on a screen thereof;

an input section for receiving an input ~~instruction determined by a user based on the screen of the display section~~ of a confirmation result of the displayed device information from a user;

a transmission ~~an authentication~~ section for transmitting the authentication response ~~executing processing of verifying or not verifying the authentication with the first communication device~~ in accordance with the result ~~instruction~~ input to the input section; and

an authentication ~~a transmission~~ section for, ~~transmitting the authentication response instructing to verify or not to verify the authentication in accordance with the result of the processing performed by the authentication section to the first communication device~~ when the device information included in the authentication response is indicative of verification of the

authentication, performing key exchange with the first communication device using the device information included in the authentication request and the authentication response.

12. (Currently Amended) A communication system for executing authentication processing for connecting a first communication device to a second communication device, wherein:

the first communication device includes:

a transmission section for transmitting an authentication request including device information indicative of ~~capable of uniquely specifying~~ the first communication device to the second communication device;

a receiving section for receiving, from the second communication device, an authentication response corresponding to the authentication request and including device information ~~corresponding to the authentication request from the second communication device~~ by which the second communication device is capable of being determined to be a source, and for monitoring and determining whether or not the authentication response is changed by an unspecified third party while being transmitted;

a display section for, when it is determined that the authentication response is not changed, displaying the device information included in the authentication response ~~request~~ on a screen thereof;

an input section for receiving an input ~~instruction determined by a user based on the screen of the display section~~ of a confirmation result of the displayed device information from a user; and

an authentication section for executing processing of verifying or not verifying the authentication with the second communication device in accordance with the result ~~instruction~~ input to the input section, and for, when the result is indicative of verification of the authentication, further performing key exchange with the second communication device using the device information included in the authentication request and the authentication response; and

the second communication device includes:

a receiving section for receiving the authentication request from the first communication device, and monitoring and determining whether or not the authentication request is changed by an unspecified third party while being transmitted;

~~an authentication section for creating the authentication response including the device information corresponding to the authentication request; and~~

a transmission section for transmitting the authentication response corresponding to the authentication request to the first communication device; and

an authentication section for, when the authentication is verified by the first communication device, performing key exchange with the first communication device using the device information included in the authentication request and the authentication response.

13. (Currently Amended) An authentication method for executing authentication processing for connecting a first communication device to a second communication device, the authentication method comprising the steps of:

the first communication device transmitting an authentication request including device

information by which the first communication device is capable of being determined to be a source ~~uniquely specifying the first communication device~~ to the second communication device;

the second communication device receiving the authentication request from the first communication device, and monitoring and determining whether or not the authentication request is changed by an unspecified third party while being transmitted;

the second communication device displaying the device information included in the authentication request on a screen thereof when it is determined that the authentication request is not changed;

the second communication device ~~inputting an instruction determined by a user based on the screen displaying the device information~~ receiving an input of a confirmation result of the displayed device information from a user;

the second communication device transmitting an authentication response including information indicative of verification or non-verification of ~~executing processing of verifying or not verifying~~ the authentication with the first communication device in accordance with the input ~~instruction~~ result;

~~the second communication device transmitting an authentication response including device information corresponding to the authentication request instructing to verify or not to verify the authentication in accordance with the result of the processing;~~

the first communication device receiving the authentication response corresponding to the authentication request from the second communication device, and monitoring and determining whether or not the authentication response is changed by an unspecified third party while being

transmitted; [[and]]

the first communication device executing processing of verifying or not verifying the authentication with the second communication device in accordance with the authentication response when it is determined that the authentication response is not changed; and

the first communication device and the second communication device performing key exchange with each other using the device information included in the authentication request and the information included in the authentication response when the information included in the authentication response is indicative of verification of the authentication.

14. (Currently Amended) An authentication method for executing authentication processing for connecting a first communication device to a second communication device, the authentication method comprising the steps of:

the first communication device transmitting an authentication request including device information indicative of ~~capable of uniquely specifying~~ the first communication device to the second communication device;

the second communication device receiving the authentication request from the first communication device, and monitoring and determining whether or not the authentication request is changed by an unspecified third party while being transmitted;

the second communication device transmitting ~~creating~~ an authentication response corresponding to the authentication request and including device information ~~corresponding to the authentication request~~ by which the second communication device is capable of being

determined to be a source to the first communication device;

~~the second communication device transmitting the authentication response to the first communication device;~~

the first communication device receiving the authentication response ~~including the device information~~ corresponding to the authentication request from the second communication device, and monitoring and determining whether or not the authentication response is changed by an unspecified third party while being transmitted;

the first communication device displaying the device information included in the authentication response ~~request~~ on a screen thereof when it is determined that the authentication response is not changed;

the first communication device ~~inputting an instruction determined by a user based on the screen displaying the device information; and~~ receiving an input of a confirmation result of the displayed device information from a user;

the first communication device executing processing of verifying or not verifying the authentication with the second communication device in accordance with the input ~~instruction~~ result; and

the first communication device and the second communication device performing key exchange with each other using the device information included in the authentication request and the authentication response when the result is indicative of verification of the authentication.

15. (New) The communication device according to claim 1, wherein the display section further displays channel information used for reception of the authentication request, in addition to the device information included in the authentication request, thereby making it possible for the user to determine whether or not the authentication request is transferred using another channel by the unspecified third party.

16. (New) The communication device according to claim 2, wherein the display section further displays channel information used for reception of the authentication response, in addition to the device information included in the authentication response, thereby making it possible for the user to determine whether or not the authentication response is transferred using another channel by the unspecified third party.

17. (New) The communication device according to claim 1, wherein the user is able to determine, based on whether or not the authentication request is received a plurality of times and whether or not a public key and a signature in the device information included in the authentication request are changed, whether or not the received authentication request is changed by the unspecified third party.

18. (New) The communication device according to claim 2, wherein the user is able to determine, based on whether or not the authentication response is received a plurality of times and whether or not a public key and a signature in the device information included in the

authentication response are changed, whether or not the received authentication response is changed by the unspecified third party.

19. (New) The communication system according to claim 11, wherein the display section further displays channel information used for reception of the authentication request, in addition to the device information included in the authentication request, thereby making it possible for the user to determine whether or not the authentication request is transferred using another channel by the unspecified third party.

20. (New) The communication system according to claim 12, wherein the display section further displays channel information used for reception of the authentication response, in addition to the device information included in the authentication response, thereby making it possible for the user to determine whether or not the authentication response is transferred using another channel by the unspecified third party.

21. (New) The communication system according to claim 11, wherein the user is able to determine, based on whether or not the authentication request is received a plurality of times and whether or not a public key and a signature in the device information included in the authentication request are changed, whether or not the received authentication request is changed by the unspecified third party.

22. (New) The communication system according to claim 12, wherein the user is able to determine, based on whether or not the authentication response is received a plurality of times and whether or not a public key and a signature in the device information included in the authentication response are changed, whether or not the received authentication response is changed by the unspecified third party.

23. (New) The authentication method according to claim 13, wherein the step of displaying the device information included in the authentication request further includes displaying channel information used for reception of the authentication request, thereby making it possible for the user to determine whether or not the authentication request is transferred using another channel by the unspecified third party.

24. (New) The authentication method according to claim 14, wherein the step of displaying the device information included in the authentication response further includes displaying channel information used for reception of the authentication response, thereby making it possible for the user to determine whether or not the authentication response is transferred using another channel by the unspecified third party.

25. (New) The authentication method according to claim 13, wherein the step of monitoring and determining whether or not the received authentication request is transmitted by the unspecified third party includes enabling the user to determine, based on whether or not the authentication

request is received a plurality of times and whether or not a public key and a signature in the device information included in the authentication request are changed, whether or not the received authentication response is changed by the unspecified third party.

26. (New) The authentication method according to claim 14, wherein the step of monitoring and determining whether or not the received authentication response is transmitted by the unspecified third party includes enabling the user to determine, based on whether or not the authentication response is received a plurality of times and whether or not a public key and a signature in the device information included in the authentication response are changed, whether or not the received authentication response is changed by the unspecified third party.